Gestion des vulnérabilités

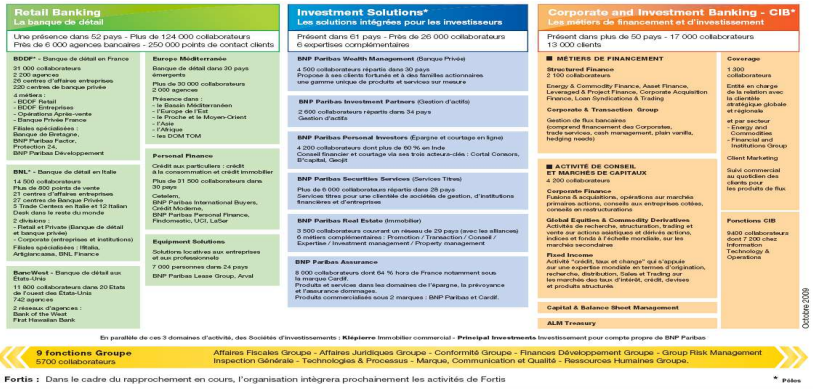
« Back to basic » ou
nouvelle tactique face à l'évolution des attaques ?

Xavier PANCHAUD
Juin 2012, Paris

Le groupe BNP Paribas

Organisation du BNP Paribas

Trois domaines d'activité, organisés en « **pôles** » ou « **entités opérationnelles** » ou « **métiers** », répartis sur différents « **territoires** » (pays ou régions).
Neuf « **fonctions** » assurent un appui transversal à l'ensemble des activités.
Les collaborateurs de ces domaines travaillent **ensemble** pour être au plus près des besoins du client.



La sécurité des SI au sein de BNP Paribas

OBJECTIF : maîtrise démontrée du risque sécurité lié aux SI conformément

- Aux lois et règlements de l'industrie bancaire et financière
- Les valeurs du groupe BNP Paribas : éthique, développement durable, valeur de la marque, maîtrise du risque opérationnel...
- L'appétence au risque propre à chaque métier dans chaque implantation

PÉRIMÈTRE : tout le groupe sur l'ensemble de ses territoires

COUVERTURE : la sécurité de l'information comme définie par l'ISO 27001

MOYENS : un cadre de management de la sécurité (politique, procédure, scorecard, gouvernance projet, veille...) et des actions permanentes

EFFECTIFS : sécurité groupe (~40 pers.) + un réseau de BISO / CISO (~30 pers.) + une communauté (~150 pers.) et des acteurs opérationnels repartis (~500 pers. soit 4% des informaticiens)

La maîtrise du risque de sécurité lié aux SI, c'est :

- Une dimension de la stratégie de Sécurité Globale
- La contribution au processus global de gestion des risques opérationnels
- Un moyen de contrôle permanent
- Une valeur du groupe BNP Paribas et de des métiers

Agenda

- **Inventaire et classification**
  - « Car nous ne pouvons protéger que ce que nous connaissons »
- **Veille**
  - « Car nous ne pouvons nous protéger que de ce que nous connaissons »
- **Patch management**
  - 0-days, ½-days et vulnérabilités humaines : lesquelles prioritiser
- **Gestion des priorités**
  - Risk acceptence et dérogation
- **Contrôle**
  - Parce que « la confiance n'exclut pas le contrôle » (Lénine)

2011 en chiffre

721 avis de sécurité

84 mises à jours majeurs

2427 mises à jours mineurs

1150 produits

9248 versions

CertIST Industrie Services Tertiaire

Inventaire et classification

« Car nous ne pouvons protéger que ce que nous connaissons »

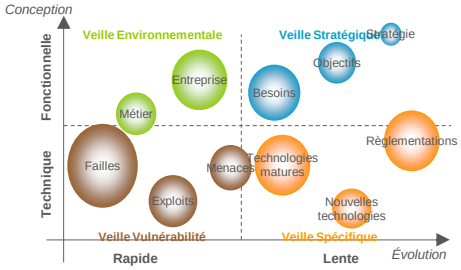
- **Un pré-requis pour :**
  - Connaître son parc
  - Identifier les priorités
  - Disposer d'état des lieux fiables

- **Souvent réduit à l'état d'objectif**
  - Limité par la taille des inventaires
  - L'indiscipline des acteurs
  - La limitation des outills

Veille

« Car nous ne pouvons nous protéger que de ce que nous connaissons »

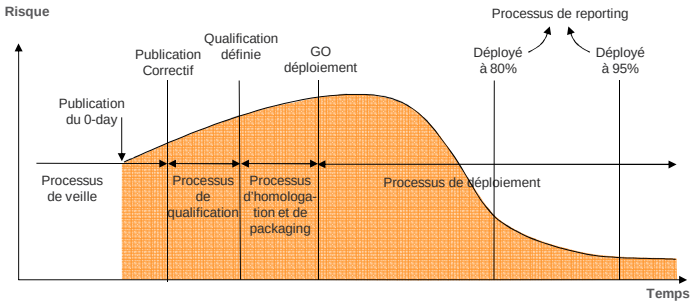
- **Indispensable sur les gros parcs**
  - **Veille Vulnérabilité**
    - Pour identifier les points faibles et les actions à réaliser
  - **Veille Environnementale**
    - Pour définir les priorités
  - **Veille Spécifique**
    - Pour anticiper



Patch management

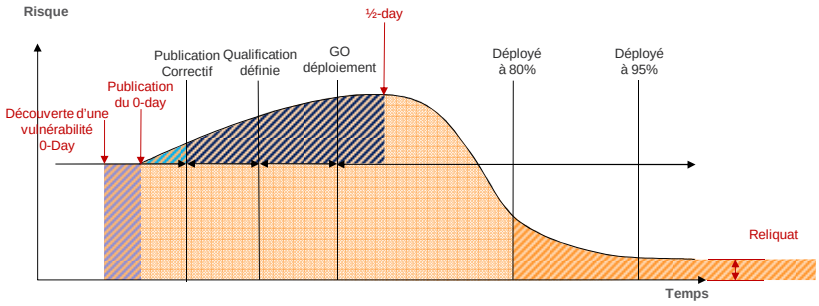
0-days, ½-days et reliquat: lesquels prioritiser

- **Rappel sur le cycle de patch-management**



La vérité sur le patch management

- **Zone de risque non maitrisable avant la connaissance du 0-day**
- **Zone de risque liée à la publication du 0-day**
- **Zone de risque subie jusqu'au patch de la moitié des équipements**
- **Zone de risque résiduelle : « reliquat »**



Gestion des priorités

- **Le patch management n'est possible que si un correctif existe**
  - Les zones de risque induites par un 0-Day doivent être gérées par des mesures de sécurité autre que le patch management
- **La zone de risque subie pendant le déploiement du correctif doit être couvertes par des mesures de sécurité complémentaires**
  - Priorisation de déploiement (actifs critiques ou très exposés)
  - Monitoring accru
- **Le risque porté par le reliquat doit continuer à être réduit**
  - Identification des équipements vulnérables non inventoriés (scans)
  - Suivi du déploiement et identification des anomalies
  - En dernier recours acceptation du risque et définition de mesures complémentaires si impossibilité de passer le correctif sur un serveur

Un processus complexe

La gestion des vulnérabilités est un processus complexe intégrant un nombre important de mesures

- **Organisationnelles**
  - Veille
  - Gestion des inventaires
  - Classification
  - Suivi du déploiement
  - Réalisation de tableaux de bord
  - Acceptation du risque
- **Techniques**
  - Détection d'événements et signatures (SMC)
  - Identification et implémentation de mesures de sécurité complémentaires
  - Déploiement de correctif
  - Scans de vulnérabilité

L'efficacité de ce processus ne peut être garanti que si toutes ces mesures sont déployées

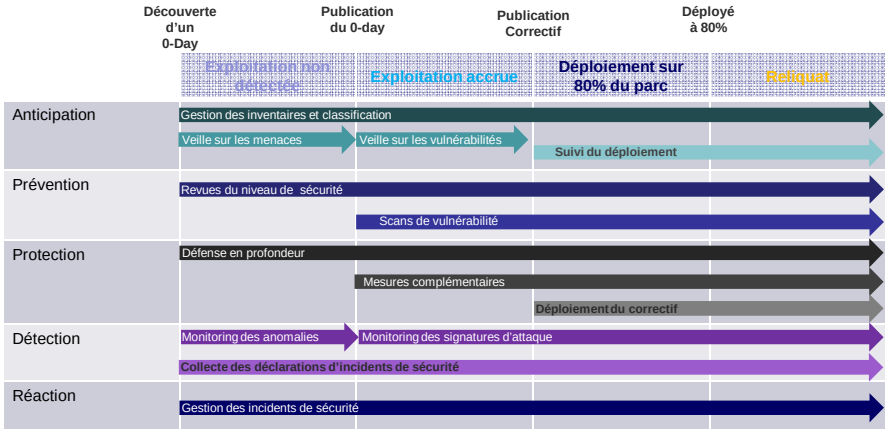
Des contrôles pour assurer l'efficacité du processus

« Implémentation » « Efficacité » « Pérennité »

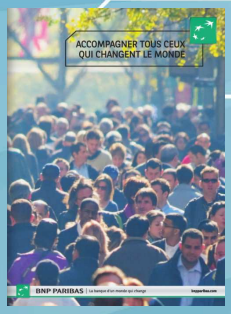
- **Trois niveaux de contrôle**
  - Contrôle de premier niveau par les équipes opérationnelles
  - Contrôle permanent par le contrôle interne
  - Contrôle périodique par l'audit interne
- **Ciblant l'ensemble du processus sécurité**
  - Du physique à l'organisation de la sécurité
  - Du technique à l'organisationnel

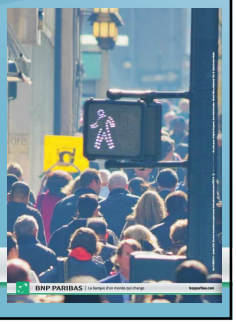
En revenant aux basiques

Une nouvelle tactique face à l'évolution des attaques : Ne pas oublier ses basiques



Questions





BNP PARIBAS | La banque d'un monde qui change